OIPE JC139 MAY 2 4 2005 PATENT & TRADEMARK OFFICE

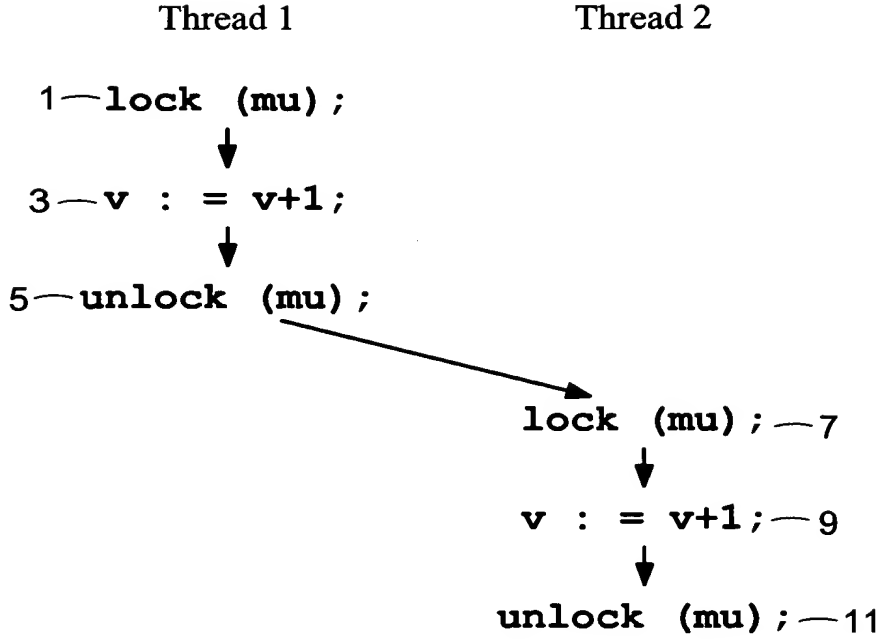

FIG. 1
PRIOR ART

Program	*locks_held*	*C(v)*
	{ }	{mu1, mu2}
101—lock (mu1);	{mu1}	
103—v := v+1;		{mu1}
105—unlock (mu1);	{ }	
107—lock (mu2);	{mu2}	
109—v := v+1;		{ }
111—unlock (mu2);	{ }	

FIG. 2
PRIOR ART

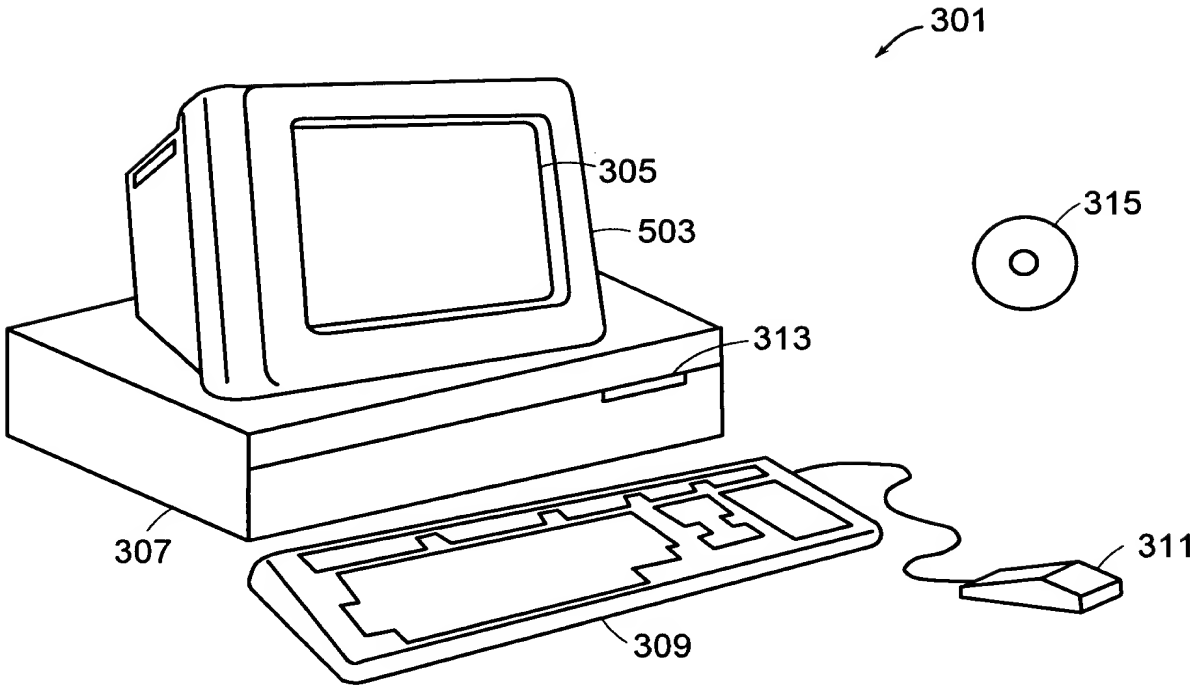

FIG. 3

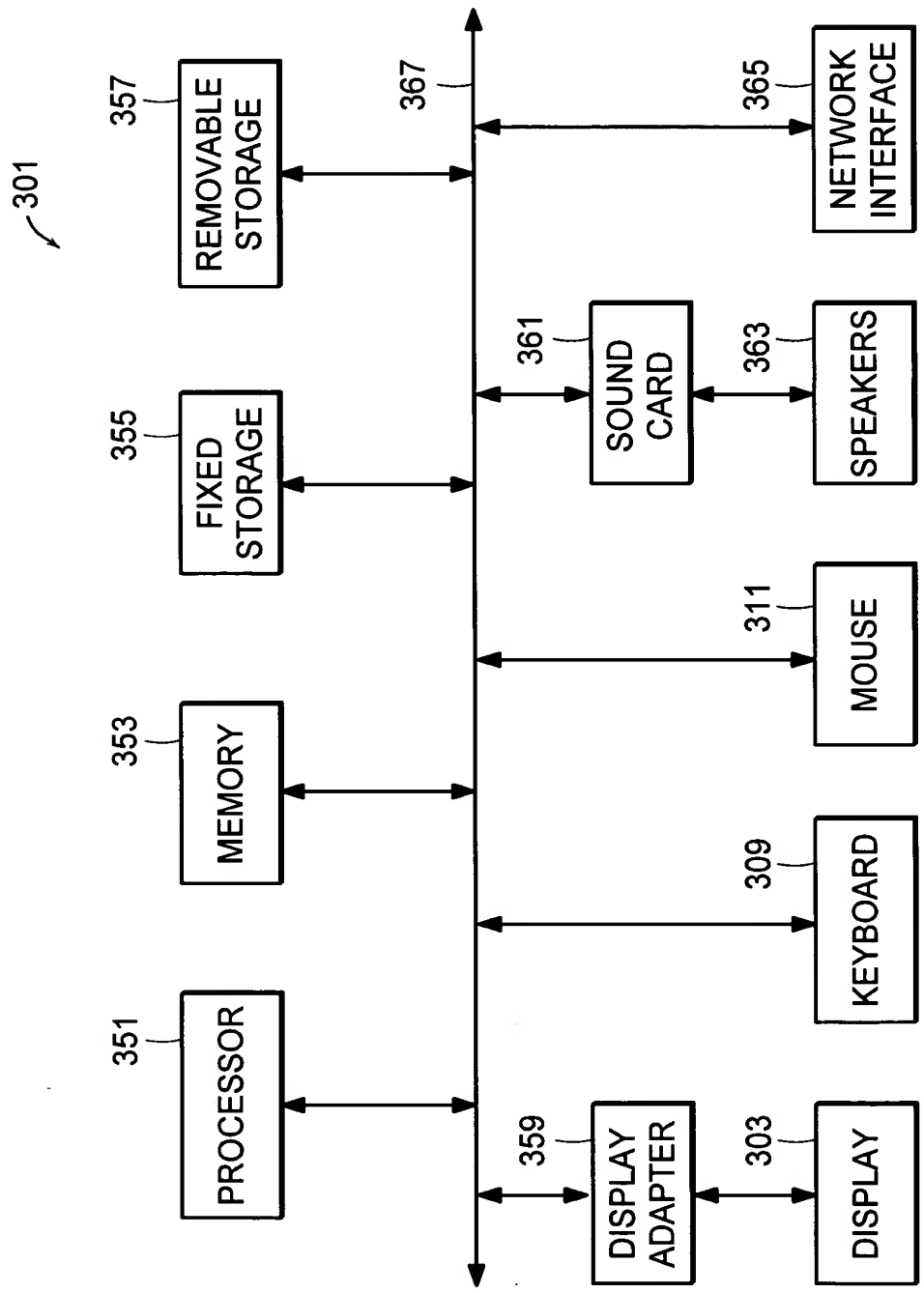
301
357
REMOVABLE STORAGE
355
FIXED STORAGE
353
MEMORY
351
PROCESSOR
367
361
SOUND CARD
359
DISPLAY ADAPTER
365
NETWORK INTERFACE
363
SPEAKERS
311
MOUSE
309
KEYBOARD
303
DISPLAY

FIG. 4

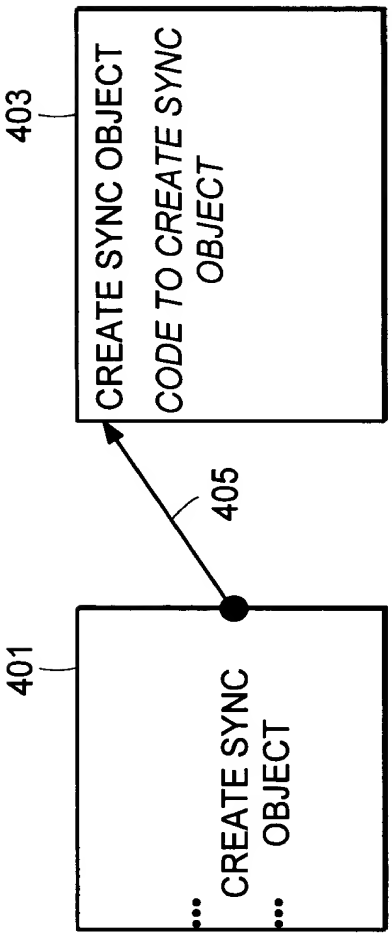
401
CREATE SYNC OBJECT
405
403
CREATE SYNC OBJECT
CODE TO CREATE SYNC OBJECT

FIG. 5A

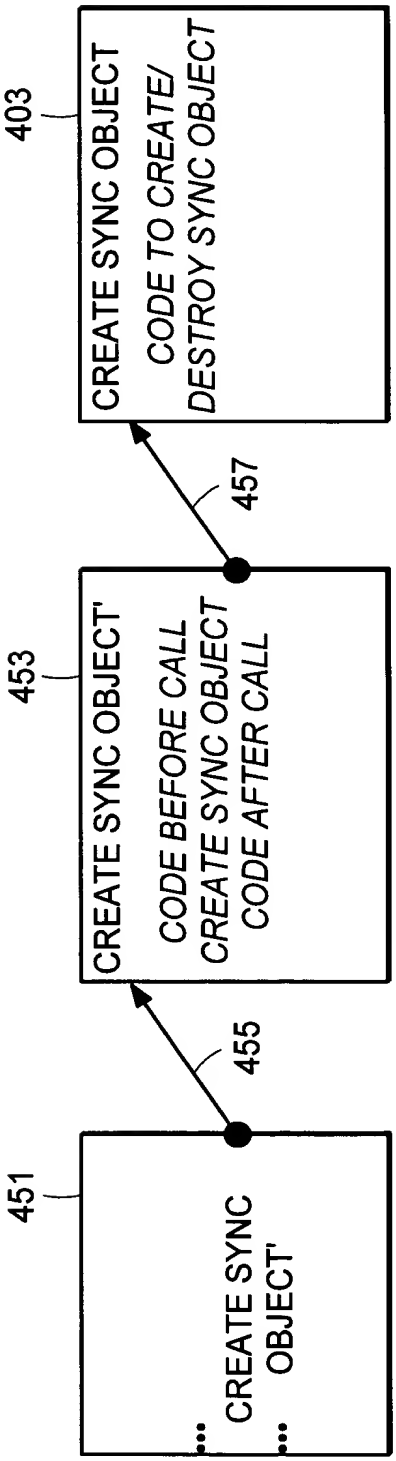
451
CREATE SYNC OBJECT'
455
453
CREATE SYNC OBJECT'
CODE BEFORE CALL
CREATE SYNC OBJECT
CODE AFTER CALL
457
403
CREATE SYNC OBJECT
CODE TO CREATE/
DESTROY SYNC OBJECT

FIG. 5B

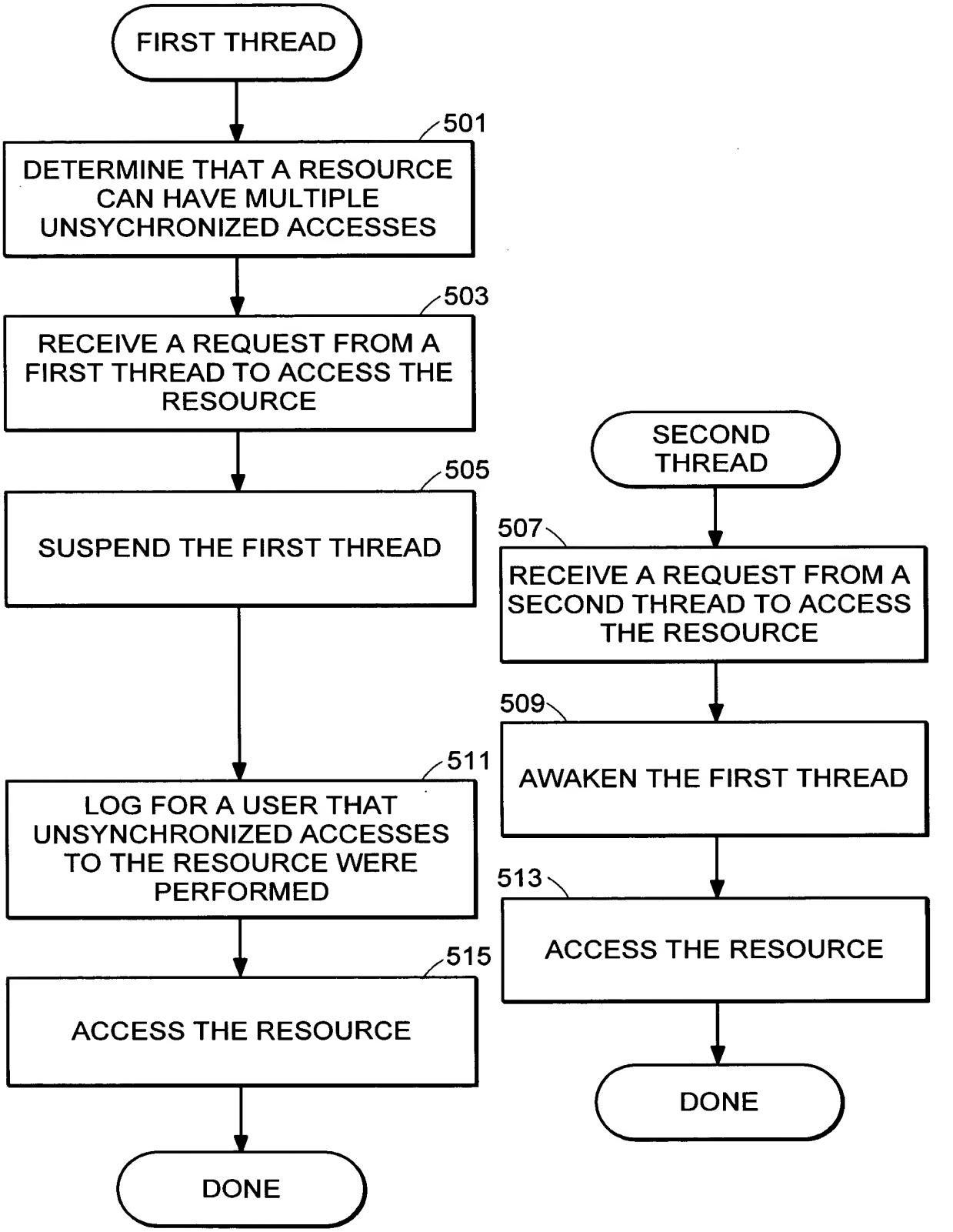
FIRST THREAD
501
DETERMINE THAT A RESOURCE CAN HAVE MULTIPLE UNSYCHRONIZED ACCESSES
503
RECEIVE A REQUEST FROM A FIRST THREAD TO ACCESS THE RESOURCE
505
SUSPEND THE FIRST THREAD
511
LOG FOR A USER THAT UNSYNCHRONIZED ACCESSES TO THE RESOURCE WERE PERFORMED
515
ACCESS THE RESOURCE
DONE
SECOND THREAD
507
RECEIVE A REQUEST FROM A SECOND THREAD TO ACCESS THE RESOURCE
509
AWAKEN THE FIRST THREAD
513
ACCESS THE RESOURCE
DONE

FIG. 6

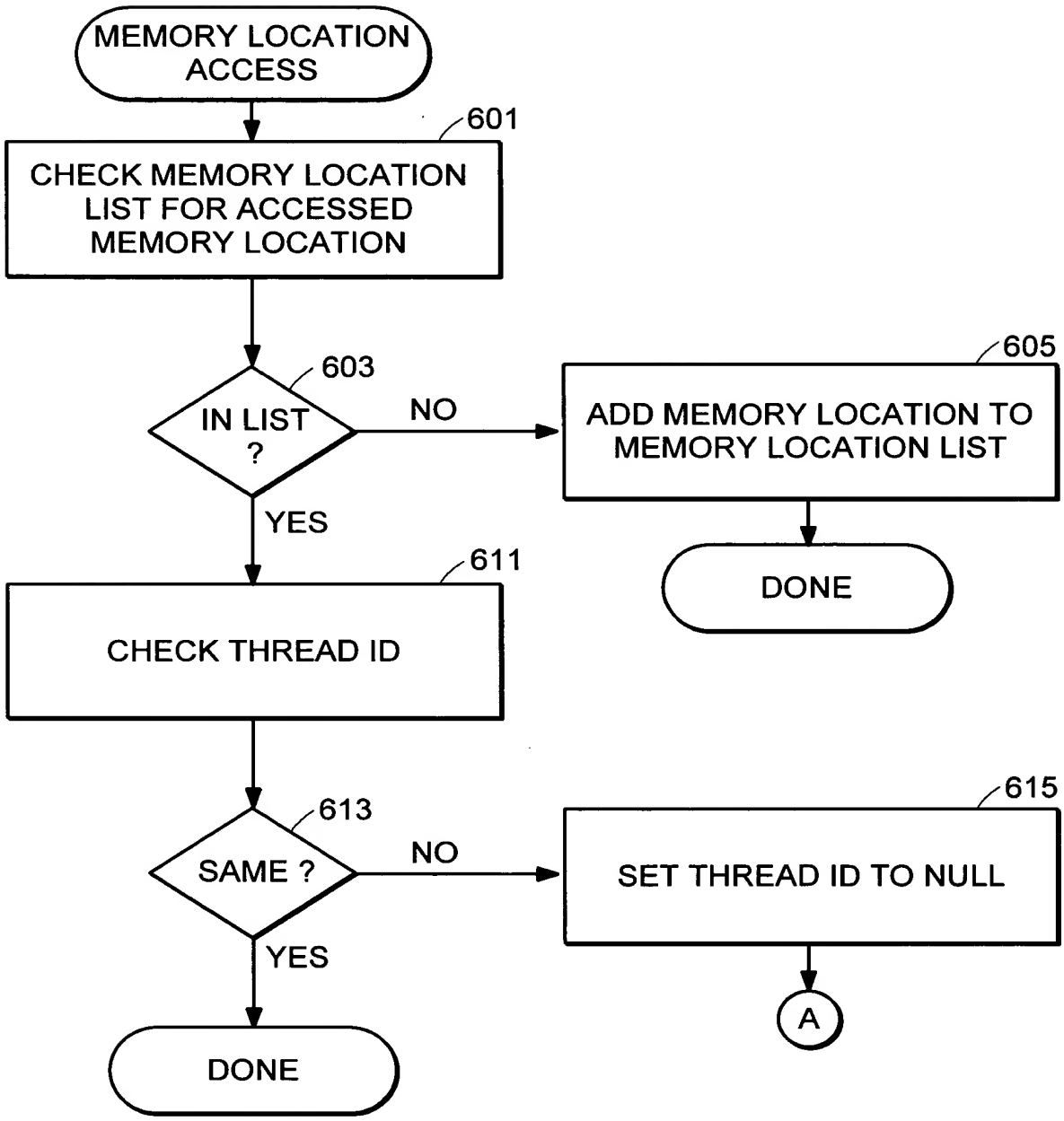
MEMORY LOCATION ACCESS
601
CHECK MEMORY LOCATION LIST FOR ACCESSED MEMORY LOCATION
603
IN LIST ?
NO
605
ADD MEMORY LOCATION TO MEMORY LOCATION LIST
DONE
YES
611
CHECK THREAD ID
613
SAME ?
NO
615
SET THREAD ID TO NULL
A
YES
DONE

FIG. 7A

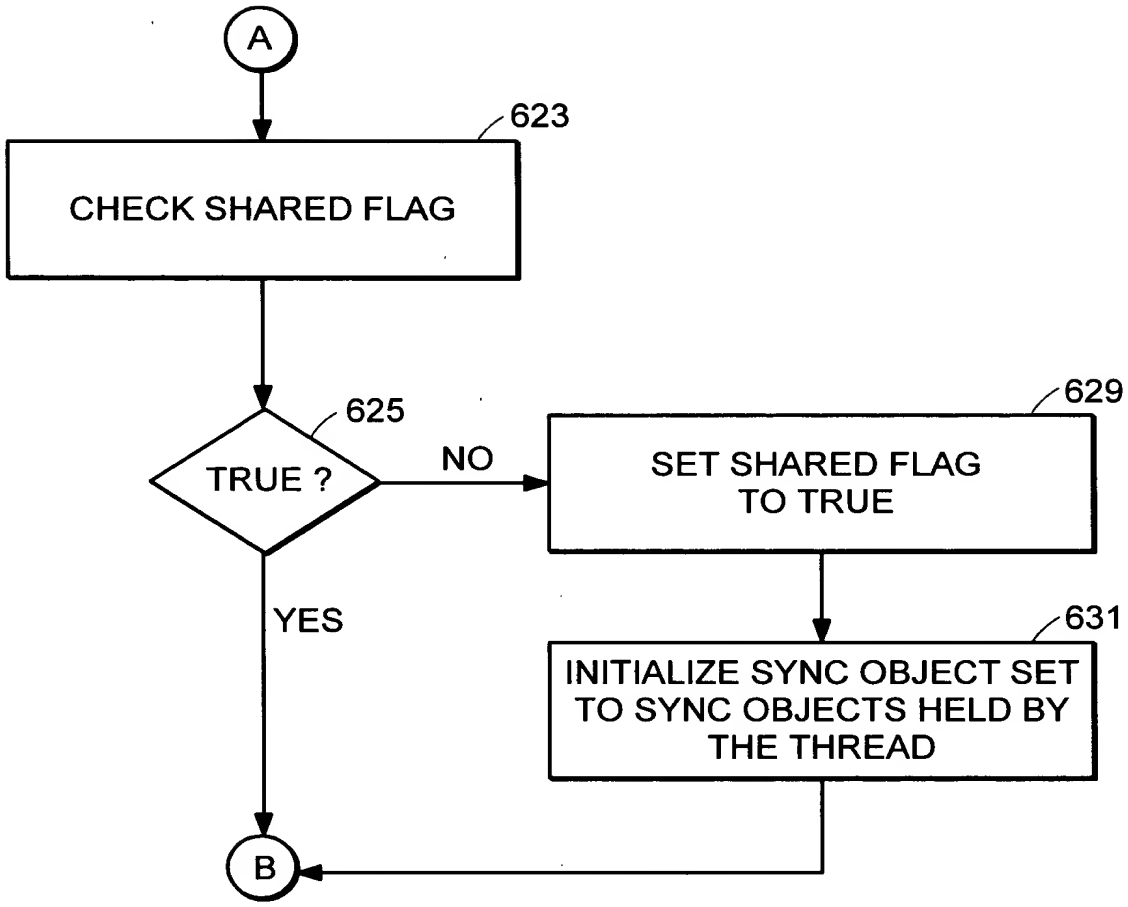
A
623
CHECK SHARED FLAG
625
TRUE ?
NO
629
SET SHARED FLAG
TO TRUE
YES
631
INITIALIZE SYNC OBJECT SET
TO SYNC OBJECTS HELD BY
THE THREAD
B

FIG. 7B

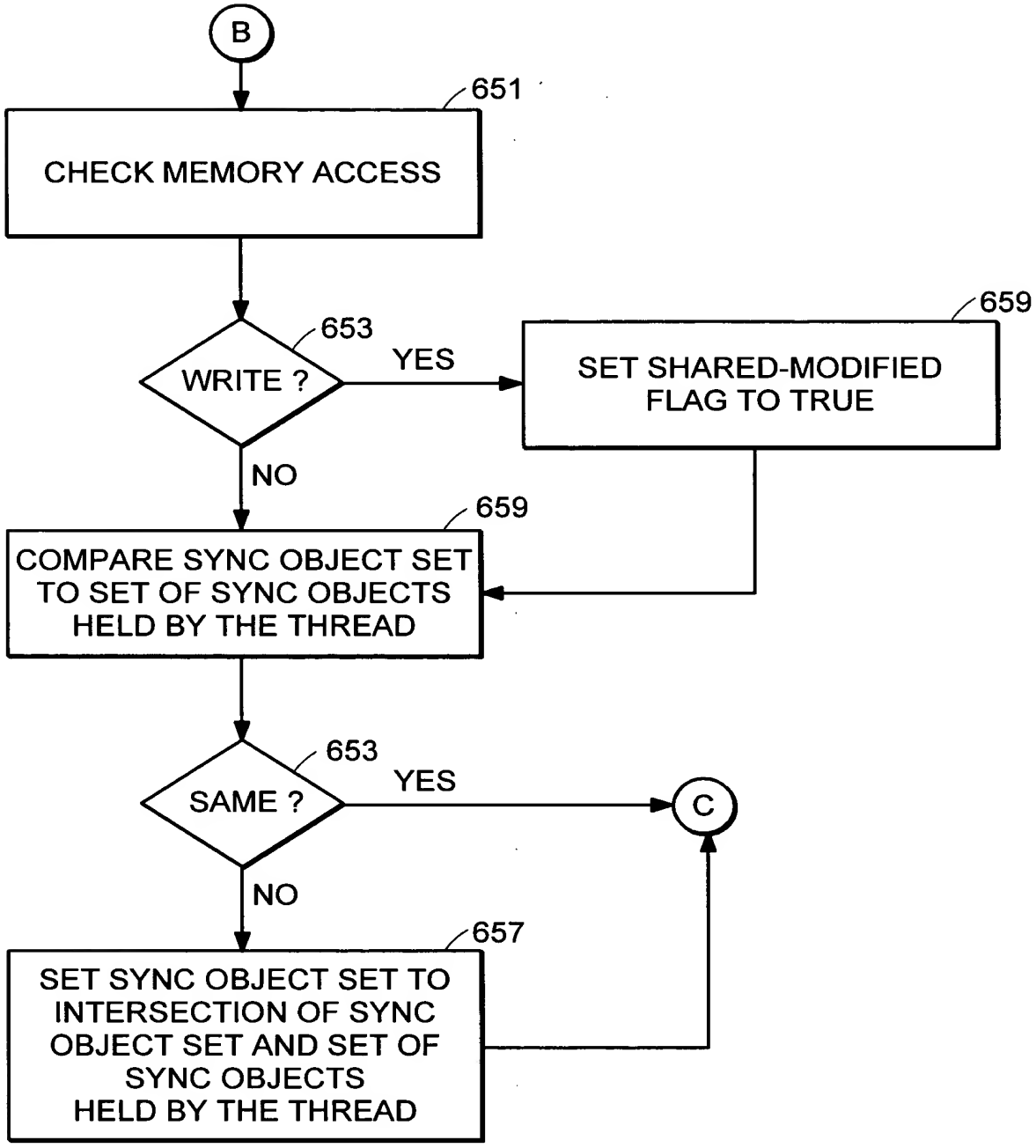
B
651
CHECK MEMORY ACCESS
653
WRITE ?
YES
659
SET SHARED-MODIFIED FLAG TO TRUE
NO
659
COMPARE SYNC OBJECT SET TO SET OF SYNC OBJECTS HELD BY THE THREAD
653
SAME ?
YES
C
NO
657
SET SYNC OBJECT SET TO INTERSECTION OF SYNC OBJECT SET AND SET OF SYNC OBJECTS HELD BY THE THREAD

FIG. 7C

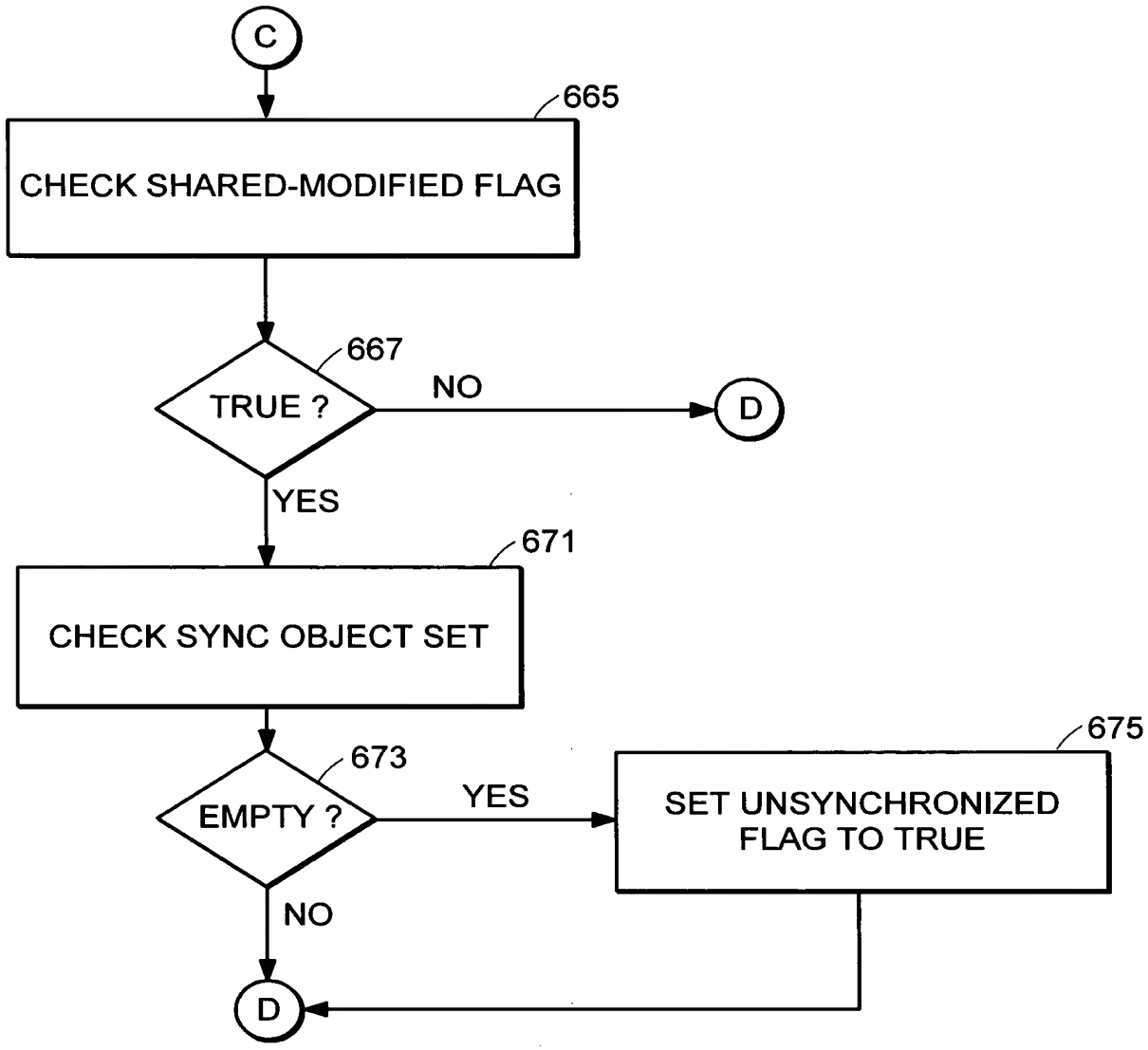
C
665
CHECK SHARED-MODIFIED FLAG
667
TRUE ?
NO
D
YES
671
CHECK SYNC OBJECT SET
673
EMPTY ?
YES
675
SET UNSYNCHRONIZED FLAG TO TRUE
NO
D

FIG. 7D

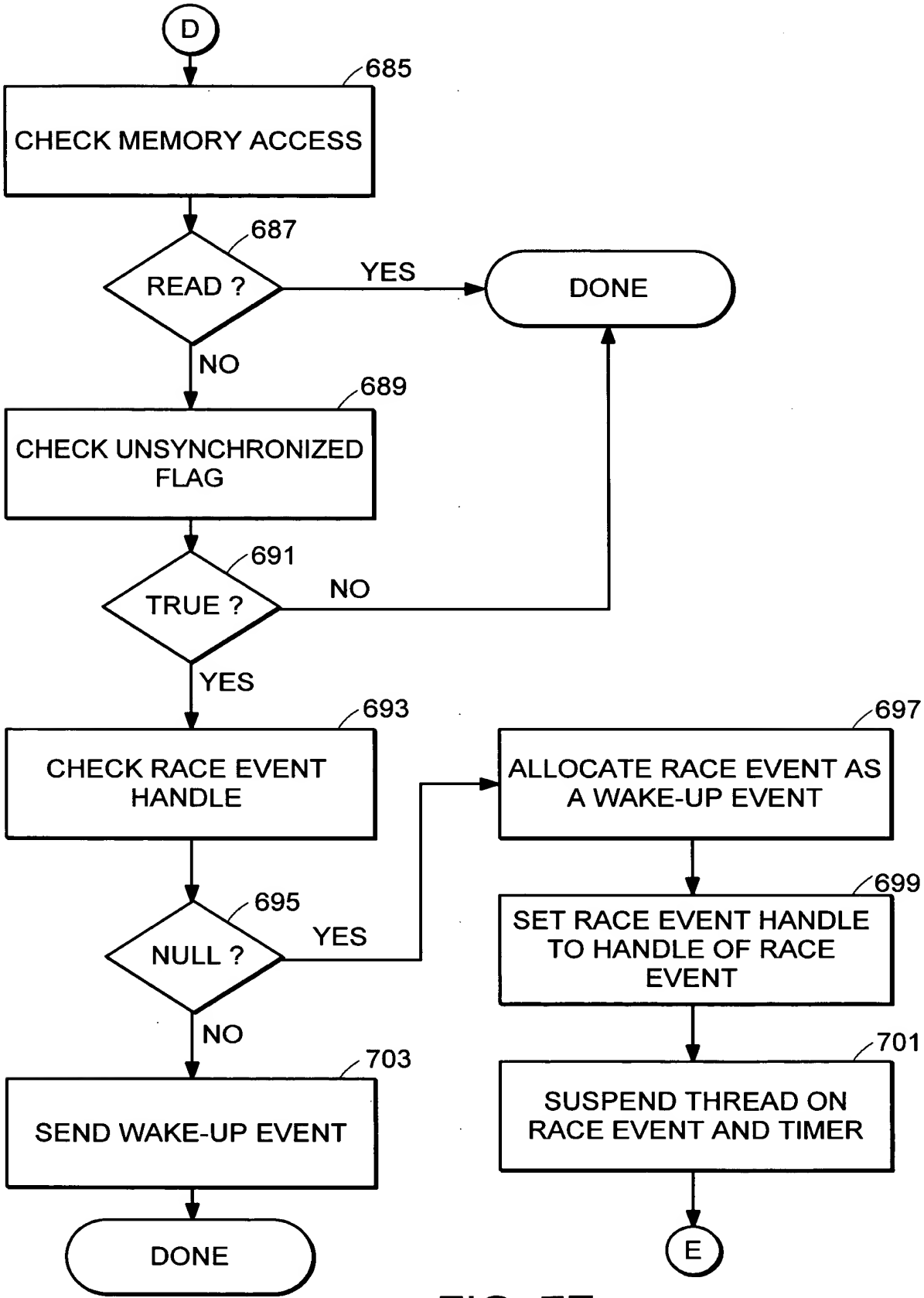
D
685
CHECK MEMORY ACCESS
687
READ ?
YES
DONE
NO
689
CHECK UNSYNCHRONIZED FLAG
691
TRUE ?
NO
YES
693
CHECK RACE EVENT HANDLE
695
NULL ?
YES
NO
703
SEND WAKE-UP EVENT
DONE
697
ALLOCATE RACE EVENT AS A WAKE-UP EVENT
699
SET RACE EVENT HANDLE TO HANDLE OF RACE EVENT
701
SUSPEND THREAD ON RACE EVENT AND TIMER
E

FIG. 7E

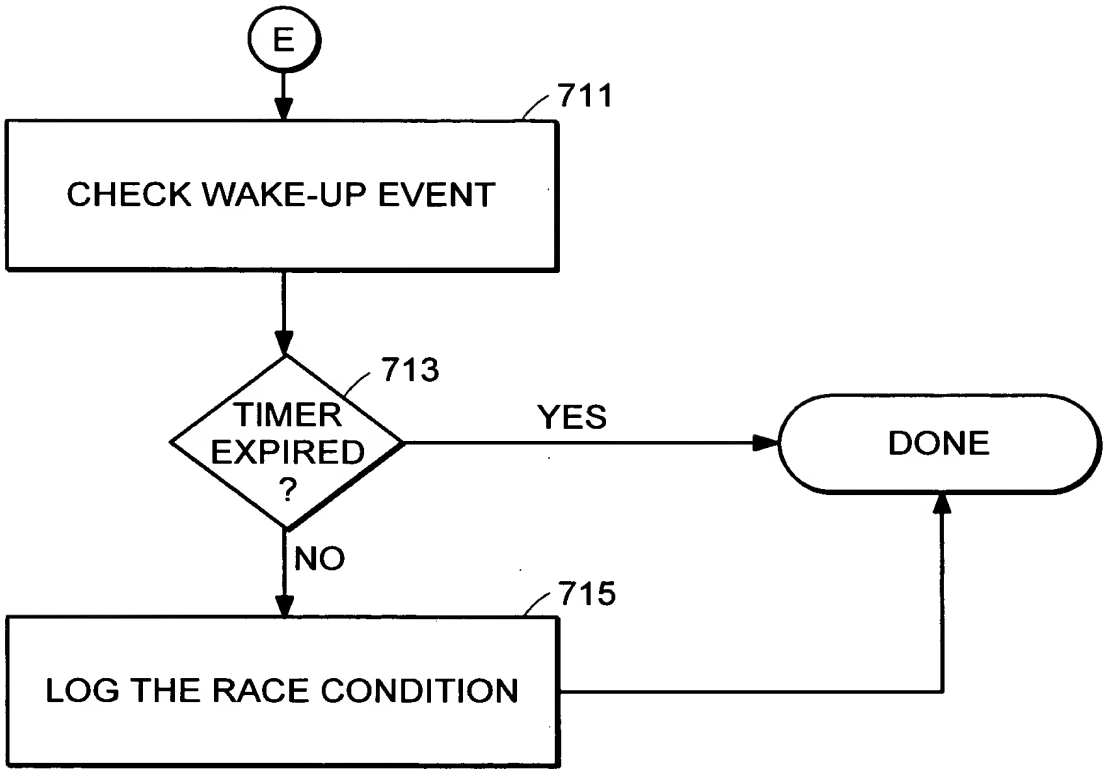
E
711
CHECK WAKE-UP EVENT
713
TIMER EXPIRED ?
YES
DONE
NO
715
LOG THE RACE CONDITION

FIG. 7F

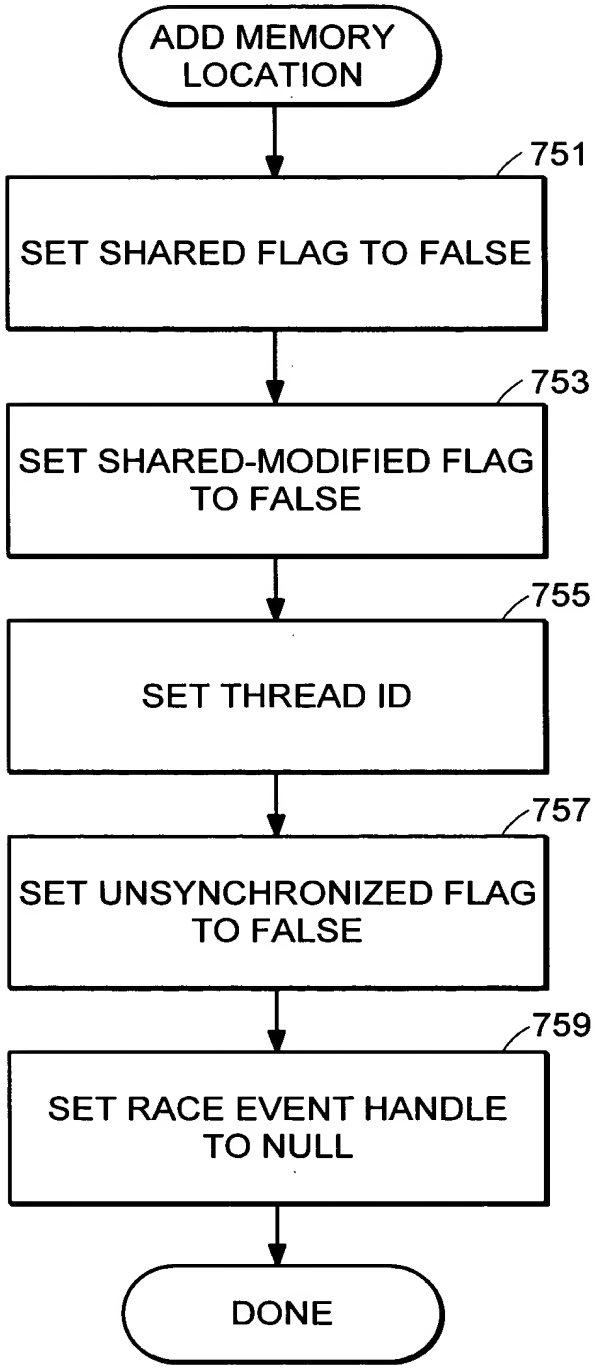
ADD MEMORY LOCATION
751
SET SHARED FLAG TO FALSE
753
SET SHARED-MODIFIED FLAG TO FALSE
755
SET THREAD ID
757
SET UNSYNCHRONIZED FLAG TO FALSE
759
SET RACE EVENT HANDLE TO NULL
DONE

FIG. 8

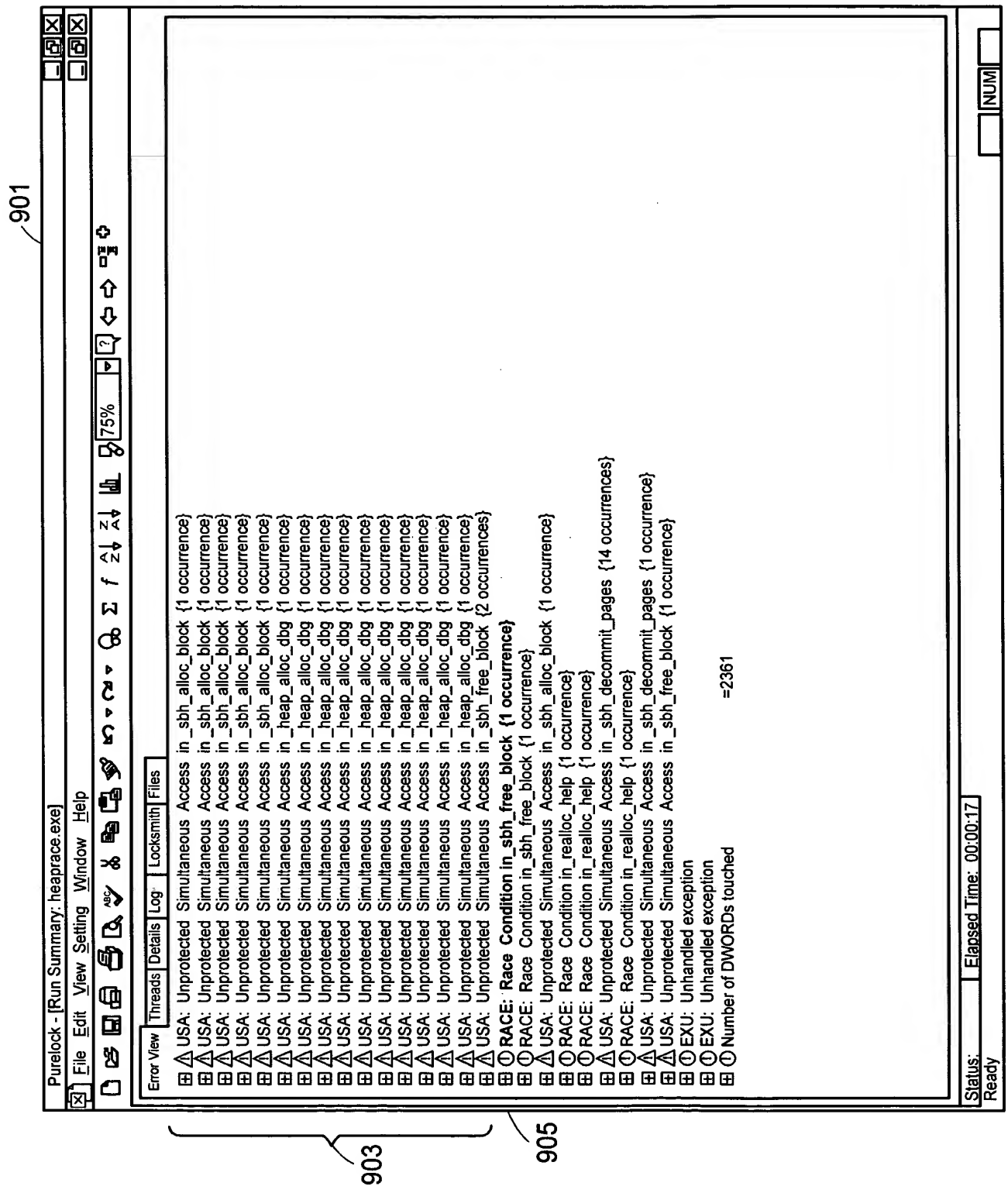
901
Purelock - [Run Summary: heaprace.exe]
File Edit View Setting Window Help
75%
Error View
Threads
Details
Log
Locksmith
Files
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _heap_alloc_dbg {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_free_block {2 occurrences}
RACE: Race Condition in_sbh_free_block {1 occurrence}
RACE: Race Condition in_sbh_free_block {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_alloc_block {1 occurrence}
RACE: Race Condition in_realloc_help {1 occurrence}
RACE: Race Condition in_realloc_help {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_decommit_pages {14 occurrences}
RACE: Race Condition in_realloc_help {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_decommit_pages {1 occurrence}
USA: Unprotected Simultaneous Access in _sbh_free_block {1 occurrence}
EXU: Unhandled exception
EXU: Unhandled exception
Number of DWORDs touched =2361
Status:
Elapsed Time: 00:00:17
Ready
NUM
903
905

FIG. 9

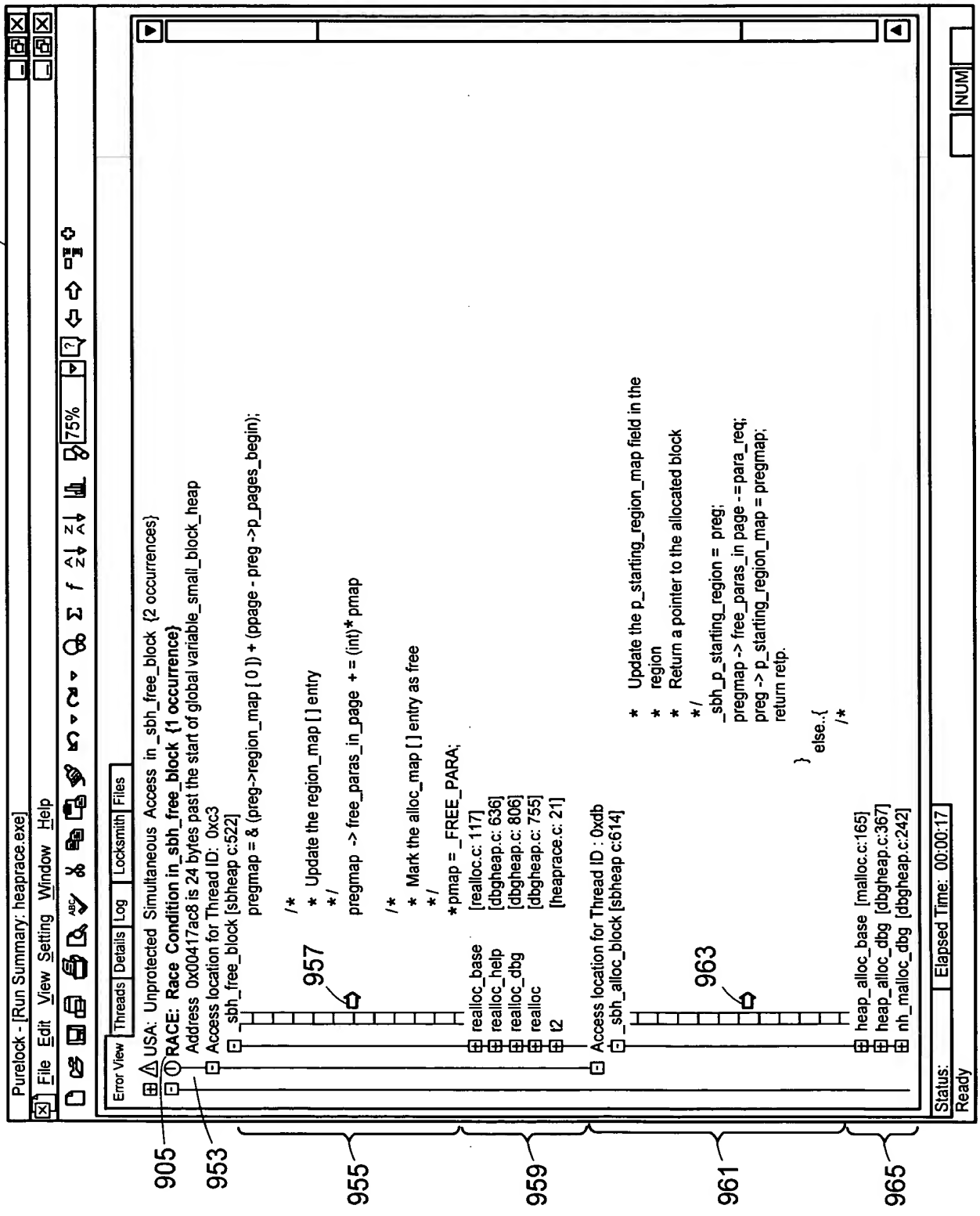
951
Purelock - [Run Summary: heaprace.exe]
File Edit View Setting Window Help
Error View Threads Details Log Locksmith Files
USA: Unprotected Simultaneous Access in _sbh_free_block {2 occurrences}
RACE: Race Condition in_sbh_free_block {1 occurrence}
Address 0x00417ac8 is 24 bytes past the start of global variable_small_block_heap
Access location for Thread ID: 0xc3
_sbh_free_block [sbheap c:522]
pregmap = & (preg->region_map [0]) + (ppage - preg ->p_pages_begin);
/*
* Update the region_map [ ] entry
*/
pregmap -> free_paras_in_page += (int)* pmap
/*
* Mark the alloc_map [ ] entry as free
*/
*pmap = _FREE_PARA;
realloc_base [realloc.c: 117]
realloc_help [dbgheap.c: 636]
realloc_dbg [dbgheap.c: 806]
realloc [dbgheap.c: 755]
t2 [heaprace.c: 21]
Access location for Thread ID : 0xdb
_sbh_alloc_block [sbheap c:614]
* Update the p_starting_region_map field in the
* region
* Return a pointer to the allocated block
*/
_sbh_p_starting_region = preg;
pregmap -> free_paras_in_page -=para_req;
preg -> p_starting_region_map = pregmap;
return retp.
}
else..{
/*
heap_alloc_base [malloc.c:165]
heap_alloc_dbg [dbgheap.c:367]
nh_malloc_dbg [dbgheap.c:242]
957
963
905
953
955
959
961
965
Status:
Elapsed Time: 00:00:17
Ready
NUM

FIG. 10